BAB I

PENDAHULUAN

1.1 Latar Belakang

Teknologi informasi menjadi kebutuhan penting bagi organisasi untuk meningkatkan kinerja organisasi. Seiring dengan kebutuhan yang semakin meningkat, perlu adanya percepatan pemenuhan sehingga tidak berdampak buruk secara luas. Informasi menjadi salah satu kebutuhan penting yang menutut ketepatan dan kecepatan dalam pemenuhannya. Informasi yang berkualitas merupakan informasi yang relevan, akurat, dan tepat waktu (Riadi et al., 2018). Hal ini membuktikan pengaruh dari pemanfaatan teknologi informasi sangat besar bagi kemajuan organisasi. Teknologi informasi menjadi solusi organisasi untuk mengumpulkan, mengolah, dan menyampaikan data menjadi informasi yang berkualitas. Namun dalam penerapannya tidak selalu terlaksana seperti yang diharapkan oleh organisasi (Riadi et al., 2018). Risiko- risiko timbul akibat hal tersebut dan dapat merugikan organisasi. Perlu adanya manajemen risiko untuk meminimalisir dampak dari kerugian risiko yang mungkin terjadi (Thenu et al., 2020).

Pada lingkungan pemerintahan, pemanfaatan teknologi informasi sangat penting untuk menjamin terlaksananya pelayanan publik dengan maksimal (Edward et al., 2019). Dinas Komunikasi dan Informatika Kota Surabaya merupakan instansi pemerintah yang memiliki tanggung jawab salah satunya pengolahan informasi dalam lingkungan pemerintahan Kota Surabaya.

Berdasarkan rencana strategis, Dinas Komunikasi dan Informatika Kota Surabaya berupaya memfasilitasi terwujudnya *good governance* melalui *electronic government (e-government)*. Penerapan prinsip *good governance* tersebut didorong dengan semakin ketatnya persaingan global yang menuntut institusi berkiprah tidak hanya dalam lingkup lokal (Dinkominfo, 2017b). Sesuai dengan misi rencana strategis yang berkaitan langsung dengan renstra Kominfo Provinsi Jawa Timur, Dinkominfo Kota Surabaya memiliki misi "memantapkan tata kelola pemerintahan yang baik melalui peningkatan layanan informasi dan pelayanan publik berbasis TIK". Ada beberapa proses yang berkaitan dengan teknologi informasi pada Dinkominfo Kota Surabaya telah memberlakukan SOP yang ditetapkan namun beberapa diantaranya masih belum optimal. Selain itu Dinkominfo Kota Surabaya juga melakukan *monitoring* dan evaluasi setiap bulannya dan pelaporan pada akhir tahun. Kegiatan yang termasuk dalam fungsi pengawasan ini, operasionalisasi diantaranya Pelaksanaan monev TIK, pelaporan hasil monev TIK, pertemuan antar koordinator dengan pemangku kepentingan layanan TI.

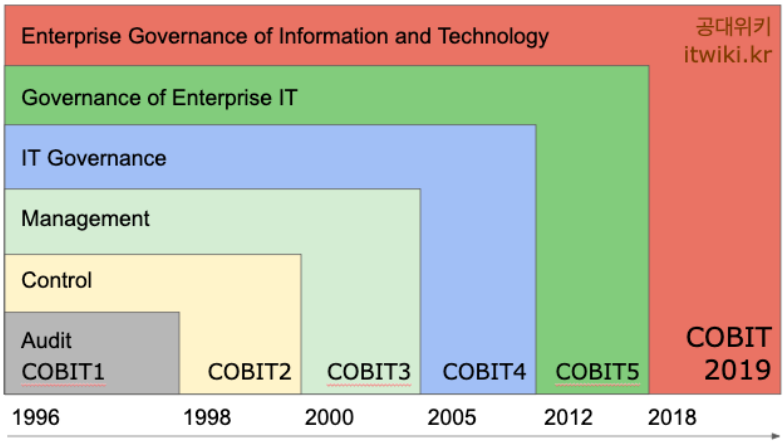
Demi meminimalisir risiko yang ada, dibutuhkan tindakan lebih dari penetapan peraturan atau SOP (Setyaningrum & Kusyanti, 2018). Hal tersebut guna menjamin optimasi risiko yang akan datang. Perlu adanya pengukuran tingkat kapabiltas untuk mengetahui sejauh mana manajemen risiko khususnya dalam keamanan informasi tekait TI yang telah dilakukan sehingga dapat menyimpulkan apakah telah diterapkan dengan cukup baik (Aziz et al., 2018). Tujuan utama dilakukan manajemen risiko adalah melindungi aset organisasi dan keterampilan penyelenggara layanan publik yang berkaitan dengan teknologi

informasi. Dinkominfo menerapkan SMKI (Sistem Manajemen Keamanan Informasi) sebagai upaya untuk melindungi aset instansi berupa informasi dan yang berkaitan. Berdasarkan hasil rekapitulasi pelaksanaan rencana kerja Dinkominfo s/d tahun 2017, terdapat 12 dokumen yang berhasil terealisasikan dari 60 dokumen yang ditargetkan untuk menjadi *outcome* dari kegiatan penyediaan sistem keamanan informasi (Dinkominfo, 2017a). Selain itu juga dilakukan penyusunan dokumen guna mendukung tata kelola e-Gov dimana hanya terdapat 1 dokumen dari 5 dokumen yang terealisasi. Hal tersebut menunjukkan jika terdapat kendala atau tantangan dalam pemenuhan target untuk memaksimalkan manajemen risiko keamanan informasi pada *e-Government* yang salah satunya Sistem Informasi Pengelolaan Surat (e-Surat). Pada tahun 2019 Dinkominfo melakukan pengukuran tingkat kapabilitas menggunakan kerangka kerja COBIT 5. Namun dalam pengukuran yang dilakukan domain pada COBIT 5 banyak yang masih berada pada *level* 1 dan *level* 2 dimana hal tersebut membuktikan jika aktivitas untuk pencapaian tata kelola yang baik belum tercapai dengan maksimal. Pengukuran tersebut hanya dilakukan secara keseluruhan pada e-Government yang berjalan, belum ada evaluasi yang secara khusus dilakukan untuk Sistem Informasi Pengelolaan Surat. Selain itu dari hasil evaluasi tersebut juga belum dapat menambahkan produk kerja yang telah ditentukan pada kerangka kerja COBIT 5. Pada penerapannya, e-Surat pernah mengalami masalah terkait kehilangan data maupun kesalahan pengiriman disposisi surat yang dapat terjadi karena kinerja server yang kurang maksimal maupun kesalahan pengguna. Sebuah standar *base practice* sangat perlu diterapkan sebagai acuan dalam melakukan pengukuran tingkat kapabilitas. Hal tersebut guna menganalisis

optimasi manajemen risiko keamanan informasi yang telah diterapkan serta dapat menjadi panduan bagi pengelola. e-Surat dipakai pada keseharian Pemerintah Kota Surabaya untuk penyampaian informasi serta disposisi kepada pihak tertuju mulai dari pengelolaan surat masuk, surat keluar, hingga pemberkasan elektronik yang membutuhkan kualitas tata kelola yang baik khususnya dalam manajemen risiko keamanan informasi. Penyampaian informasi diharapkan dapat terjaga sampai pada tujuan untuk mencegah penyebaran informasi sensitif yang berisiko menghambat kinerja Pemerintah Kota Surabaya. Terdapat beberapa kerangka kerja tata kelola TI yang dapat digunakan seperti COBIT, ISO 27001, dan ITIL (Rochmania et al., 2020).

Pada studi kasus ini kerangka kerja yang digunakan untuk mengukur tingkat kapabilitas manajemen risiko keamanan informasi adalah COBIT 5. *Control Objectives for Information and Related Technology* merupakan kerangka kerja yang menyediakan pedoman atau *base practice* bagi manajerial TI dalam mengelola organisasi seperti: *executive summary, framework, control objectives, audit guidelines, implementation tool set*, dan *management guidelines*. COBIT dikembangkan oleh lembaga ITGI (*IT Governance Institute*) yang merupakan bagian dari ISACA (*System Information and Control Association*). Kerangka kerja COBIT membantu pengguna, manajemen, dan auditor untuk menjembatani kesenjangan antara risiko bisnis, kebutuhan kontrol, dan permasalahan teknis yang berhubungan dengan teknologi informasi. Perkembangan tata kelola TI semakin luas seiring dengan kebutuhan TI yang meningkat. Terdorong dari hal tersebut, COBIT telah melewati beberapa generasi mulai dari tahun 1996 yang diterbitkan untuk pertama kalinya COBIT 1 berfokus hanya pada audit hingga

tahun 2018 yang berhasil mengembangkan COBIT 2019 yang lebih kompleks daripada generasi sebelumnya. Cakupan COBIT dari setiap generasinya memiliki perbedaan dan batasannya masing- masing. Hal tersebut menyesuaikan kebutuhan serta kondisi dari perkembangan dunia teknologi informasi. Evolusi perkembangan COBIT ada pada Gambar 1.1 berikut.



Gambar 1.1 Evolusi COBIT (Itwiki, 2020)

Salah satu generasi terbaru dari COBIT yang berhasil dikembangkan pada tahun 2012, COBIT 5 merupakan framework yang dirancang untuk mengukur kualitas sebuah tata kelola TI agar lebih fokus pada *IT strategic value* dan memastikan implementasi teknologi informasi mendukung tercapainya visi dan misi institusi. COBIT 2019 yang diluncurkan pada tahun 2018 bersifat lebih *flexible* jika dibandingkan dengan generasi sebelumnya (Syuhada, 2021). Prinsip dan rincian domain lebih kompleks sehingga lebih sulit untuk diimplementasikan. Jumlah studi pustaka mengenai COBIT 2019 dalam pengukuran tata kelola TI terbatas. Maka dari itu diputuskan penelitian ini menggunakan COBIT 5 sebagai kerangka kerja pengukuran untuk mendukung implementasi tata kelola yang komprehensif dan sistem manajemen terkait teknoogi informasi.

Pada kurun 2014 hingga 2018 dari domain Indonesia dan luar negeri, jumlah penelitian yang terpublikasi didominasi oleh kerangka kerja COBIT (Rochmania et al., 2020). Sedangkan untuk penggunaan kerangka kerja ISO 27001 dan *Information Technology Infrastructure Library* (ITIL) berada di bawah posisi jumlah penggunaan COBIT. ISO 27001 mengarah pada pengukuran mutu organisasi dan hanya bersifat teknis(Sahibudin & Ayat, 2008). Dalam kasus keamanan informasi standar ISO memang banyak digunakan namun dalam pembahasan manajemen risiko, ISO hanya sampai pada mengontrol dan mengurangi risiko untuk menghindari meningkatnya biaya yang tidak dibahas secara komprehensif jika dibandingkan dengan ITIL dan COBIT yang memberikan panduan batasan biaya manajemen risiko yang efektif dan aspek keuangan yang berkaitan dengan IT (Wibowo et al., 2016). ITIL berfokus pada *service quality* atau pelayanan pelanggan. CSF yang ada dalam metodologi COBIT mengatasi lebih banyak aspek dibandingkan dengan ITIL dan ISO. Fokus manajemen teknologi informasi dimiliki oleh *framework* COBIT. Kerangka kerja COBIT memiliki prinsip- prinsip yang tidak dimiliki oleh *framework* lainnya (Rochmania et al., 2020). COBIT digunakan untuk melakukan evaluasi secara kritis pada keberhasilan faktor, metrik, indikator dan audit (Wibowo et al., 2016).

COBIT 5 mengintegrasikan semua pengetahuan yang sebelumnya tersebar di berbagai *framework* berbeda. Kerangka kerja COBIT 5 menyatukan panduan ISACA yang ada yaitu COBIT 4.1, Val IT 2.0, Risk IT, dan BMIS serta menyesuaikan antara *base practices* yang ada seperti ITIL V3, TOGAF dan ISO (ISACA, 2012). Dalam COBIT 5 terdapat 5 domain dengan 37 proses dan secara rinci memberikan Batasan antara tata kelola TI dan manajemen TI (ISACA,

2012). Pada area tata kelola terdapat satu domain yaitu *Evaluate, Direct and Monitor* (EDM). Sedangkan pada area manajemen terdapat empat domain yaitu *Align, Plan and Organize* (APO), *Build, Acquire and Implement* (BAI), *Deliver, Service and Support* (DSS), dan *Monitor, Evaluate and Assess* (MEA). Pengelolaan risiko terdapat pada subdomain EDM03 dan APO12. Subdomain EDM03 berada pada area tata kelola yang akan memastikan bahwa terdapat optimasi risiko yang diterapkan pada instansi. Sedangkan subdomain APO12 berada pada area manajemen yang berfungsi untuk mengelola risiko yang ada pada instansi.

Berdasarkan penelitian- penelitian sebelumnya yang mengangkat masalah yang sama terkait manajemen risiko keamanan informasi, banyak mengadopsi COBIT 5 sebagai kerangka kerja dalam pengukuran tingkat kapabilitas. Studi terkait yang pernah dilakukan oleh Fransisca bertujuan untuk mengetahui tingkat kapabilitas dalam memastikan optimasi risiko manajemen keamanan informasi yang telah dilaksanakan Organisasi XYZ menggunakan *framework* COBIT 5 pada subdomain EDM03 (*Ensure Risk Optimation*). Selain itu, studi yang dilakukan oleh Arief juga bertujuan untuk mengukur tingkat kapabilitas manajemen risiko Sistem Informasi Koperasi Syariah di KSPPS XYZ, tingkat kapabilitas yang ditargetkan, dan memberikan kontribusi untuk perbaikan dari masalah yang ditemukan dengan menggunakan *framework* COBIT 5 pada subdomain EDM03 dan APO12. Penelitian ini mengacu pada salah satu *Stakeholder Needs* dalam COBIT 5 *Goals Cascade* yaitu *Risk Optimation* serta salah satu fokus area tata kelola TI yaitu *manage risk.* Dimana fokus yang diambil yaitu manajemen risiko keamanan informasi yang mengacu pada pentingnya penyampaian informasi dan

disposisi kepada pihak yang dituju dalam Pemerintahan Kota Surabaya. Judul penelitian yang diajukan adalah **"Pengukuran Tingkat Kapabilitas Manajemen Risiko Keamanan Informasi pada Sistem Informasi Pengelolaan Surat menggunakan Kerangka Kerja COBIT 5"**.

1.2 Rumusan Masalah

Berdasarkan latar belakang yang telah dipaparkan, rumus masalah dalam penelitian ini sebagai berikut :

a. Berapa tingkat kapabilitas manajemen risiko keamanan informasi Sistem Informasi Pengelolaan Surat Dinas Komunikasi dan Informatika Kota Surabaya berdasarkan kerangka kerja COBIT 5?
b. Apakah terdapat kesenjangan antara kondisi saat ini dengan kondisi yang diharapkan untuk manajemen risiko keamanan informasi Sistem Informasi Pengelolaan Surat Dinas Komunikasi dan Informatika Kota Surabaya?
c. Apa rekomendasi perbaikan manajemen risiko keamanan informasi pada Sistem Informasi Pengelolaan Surat dari hasil pengukuran tingkat kapabilitas?

1.3 Batasan Masalah

Terdapat beberapa batasan masalah pada penyusunan proposal skripsi ini, diantaranya yaitu :

a. Pengukuran tingkat kapabilitas berfokus pada tujuan bisnis EG15 *Compliance with internal policies* dimana proses yang terpilih yaitu EDM03 (*Ensure Risk Optimisation*) dan APO12 (*Manage Risk*) pada kerangka kerja COBIT 5.
b. Lembaga yang menjadi studi kasus adalah Dinas Komunikasi dan Informatika Kota Surabaya.
c. Manajemen risiko tertuju pada keamanan informasi Sistem Informasi Pengelolaan Surat (E-Surat) Dinas Komunikasi dan Informatika Kota Surabaya disesuaikan dengan tujuan TI dalam COBIT 5 yaitu ITRG10 *Security of Information, processing, infrastructure, and application*.
d. Pengukuran tingkat kapabilitas manajemen risiko mengacu pada kerangka kerja COBIT 5 dan Kebijakan Pemerintahan Kota Surabaya.

1.4 Tujuan

Adapun tujuan dari penelitian ini yaitu :

a. Mengetahui tingkat kapabilitas manajemen risiko keamanan informasi Sistem Informasi Pengelolaan Surat (E-Surat) Dinas Komunikasi dan Informatika Kota Surabaya.

b. Mendapatkan nilai kesenjangan antara kondisi saat ini dengan kondisi yang diharapkan dari penerapan manajemen risiko keamanan informasi Dinas Komunikasi dan Informatika Kota Surabaya.
c. Memberikan rekomendasi perbaikan untuk meningkatkan manajemen risiko Sistem Informasi Pengelolaan Surat (E-Surat) Dinas Komunikasi dan Informatika Kota Surabaya.

1.5 Manfaat

Beberapa manfaat yang diharapkan dari penelitian skripsi ini diantaranya :

a. Bagi Dinas Komunikasi dan Informatika Kota Surabaya diharapkan dapat membantu untuk mengetahui tingkat capaian dari penerapan manajemen risiko keamanan informasi pada e-Surat. Rekomendasi yang dihasilkan dari penelitian ini dapat menjadi bahan pertimbangan ataupun tolak ukur untuk peningkatan manajemennya.
b. Bagi Akademis penelitian ini diharapkan dapat menjadi refrensi penelitian selanjutnya terkait COBIT 5 dan sekaligus sebagai wujud kontribusi ilmu pengetahuan dari apa yang selama ini telah dipelajari selama perkuliahan di Program Studi Sistem Informasi UPN “Veteran” Jawa Timur terutama dalam bidang minat Manajemen Sistem Informasi.

1.6 Relevansi Audit Sistem Informasi dengan Sistem Informasi

Tata kelola teknologi informasi merupakan bagian penting yang tidak dapat terpisahkan bagi sebuah perusahaan. Pemanfaatan TI menjadi salah satu faktor penting untuk meraih tujuan perusahaan. Mengambil dari pernyataan ITGI (*IT Goverment Insitute)* pada tahun 2003, tata kelola TI merupakan bagian dari tata kelola perusahaan yang terdiri dari kepemimpinan, struktur organisasi, dan proses demi memastikan keberlanjutan organisasi TI dan pengembangan strategi dan tujuan organisasi. Tata kelola TI berperan untuk mengintegrasikan serta mengoptimalisasikan metode untuk merencanakan, mengorganisasikan, melaksanakan akuisisi dan implementasi, *delivery* dan *support*, serta monitoring dan evaluasi kinerja TI.

Demi menjamin tata kelola TI yang baik perlu dilakukannya audit yang salah satu fungsinya dapat menganalisis tingkat kapabilitas dari pengelolaan sistem serta teknologi informasi yang telah diterapkan perusahaan. Selain itu, menurut salah satu hasil kesepakatan dari pertemuan pertama Forum Pimpinan Program Studi Sistem Informasi se-Indonesia yang membahas terkait disiplin ilmu Sistem Informasi sekaligus ruang lingkupnya menyatakan bahwa salah satu aspek disiplin ilmu Sistem Informasi adalah Evaluasi/ Audit Sistem Informasi(Forum Pimpinan Prodi Sistem Informasi se-Indonesia, 2018). Menurut Ron Weber (1999), Audit sistem informasi merupakan proses pengumpulan dan penilaian bukti-bukti untuk menentukan apakah sistem komputer dapat mengamankan aset, memelihara integritas data, dapat mendorong pencapaian tujuan organisasi secara efektif dan menggunakan sumberdaya secara efisien. Kemudian menurut Alvin A. Arens dan James K. Loebbecke (2006), Audit sistem

informasi adalah pengumpulan dan evaluasi terhadap bukti untuk menentukan derajat kesesuaian antar informasi dan kriteria yang telah ditetapkan. Hal ini berarti dalam pelaksanannya evaluasi dilakukan mengacu pada sejumlah kriteria tertentu untuk menentukan derajat kinerja yang telah dicapai. Audit Sistem Informasi merupakan irisan dari disiplin ilmu Sistem Informasi.

1.7 Sistematika Penulisan

Pembahasan penelitian dalam proposal skripsi ini disajikan dalam lima bab dengan sistematika sebagai berikut :

BAB I PENDAHULUAN

Pendahuluan berisi latar belakang, rumusan masalah, batasan masalah, tujuan penelitian, dan sistematika penulisan yang digunakan dalam penelitian di Dinas Komunikasi dan Informatika Kota Surabaya.

BAB II TINJAUAN PUSTAKA

Pada bab ini akan menjelaskan profil singkat dari Dinas Komunikasi dan Informatika Kota Surabaya dan Sistem Informasi Pengelolaan Surat (e-Surat) serta dasar teori yang menjadi acuan penelitian yang membahas mengenai tata kelola teknologi informasi, manajemen risiko keamanan informasi, COBIT 5, analisis kesenjangan dan beberapa penelitian terdahulu.

BAB III METODOLOGI PENELITIAN

Bab ini memparkan secara urut dan sistematis langkah- langkah serta metode yang digunakan dalam penelitian sebagai pedoman dalam menyelesaikan masalah yang diangkat.

BAB IV HASIL DAN PEMBAHASAN

Bab ini menjelaskan secara rinci hasil dari setiap langkah pada metodologi penelitian dan membahasnya secara sistematis pengukuran tingkat kapabilitas manajemen risiko keamanan informasi e-Surat berdasarkan COBIT 5.

BAB V KESIMPULAN DAN SARAN

Bab ini memuat simpulan dari hasil penelitian yang telah dilakukan dan saran untuk penelitian kedepan.

DAFTAR PUSTAKA

Bagian ini merupakan daftar dari beberapa sumber literatur seperti jurnal, buku, dan situs web yang digunakan dalam penyusunan proposal skripsi ini.

LAMPIRAN

Bagian lampiran memuat informasi baik dokumen maupun bukti gambar yang digunakan untuk mendukung dan melengkapi isi dari penelitian.